Szabadság, jog és szabályozás a kibertérben

Fekete László

A digitális kultúra avantgárdja a kezdetektõl fogva ellenérzéssel és gyanakvással fogadta az államok, a nemzetközi politikai és gazdasági szervezetek azon törekvéseit, hogy a világháló mûködését kívülrõl diktált szabályok közé kényszerítsék. Az ott folyó kommunikációnak ugyanis vannak már írott és íratlan szabályai. Ezeket a technikai és közösségi szabályokat – a számítógépeket és lokális hálózatokat összekapcsoló TCP/IP protokolltól az országkódokon és generikus kódokon alapuló legfelsõbb szintû tartományneveken át a tisztességes számítógép-használat és kommunikáció chartájáig – önkéntesek alkották meg, és azok a használók konszenzusán alapulnak. Hiszen a világhálónak nem volt és ma sincs kormánya, amely különleges autoritásánál fogva bármit is rákényszeríthetne annak közösségére. Ezek a szabályok persze a világháló létrehozóinak és elsõ néhány százezer használójának politikai kultúráját, értékvilágát fejezik ki, amely világosan és egyértelmûen felismerhetõ az általuk teremtett és egymás között használt beszédmódban. Ha szavakat kellene keresnünk a digitális kultúra értékvilágának a jellemzésére, akkor elõször a nyitottság, a középpont-nélküliség, az interaktivitás, a konszenzuson alapuló szabályozás, a szabad identitásválasztás, a nem lokalitás, a hierarchia, az elõjogok és a tekintélyek elutasítása jut az eszünkbe. A digitális kultúra létrehozói szerint ezek a szavak jelölik ki tudásunk, kultúránk, emberi kapcsolataink és politikai cselekvéseink új horizontját. Az internet nagy hatású teoretikusai ezért is szeretik önmagukat és a világháló társadalmát úgy látni, mint akik Jefferson, Washington, Paine, Mill, Madison, Tocqueville, Brandeis, Holmes és mások libertinus politikai filozófiai hagyományait folytatják, azokat radikalizálják és teljesítik ki a kibertérben (Barbrook és Cameron 1997: 41–59; Barlow 1990: 45–57; Sobchack 1995: 11–28; Sterling 1994).

Mivel a világháló nem más, mint az emberek, valamint az emberek és a gépek közötti kommunikáció hálójában létrehozott tranzakciók, kapcsolatok és gondolatok halmaza, ezért pillanatról pillanatra igényli a használók – akik egyben létrehozók – millióinak virtuális jelenlétét. Lényegébõl következõen participatorikus. A világháló mint közös terv nem jöhetett volna létre s nem is maradhatna fenn a használók-létrehozók személyes elkötelezettsége, aktív részvétele és konszenzusa nélkül, ami egyszerûen azt jelenti, hogy bekapcsolódnak az ott zajló gigantikus párbeszédbe, tekintettel vannak a kommunikáció szabályaira, és lehetõségeik szerint

maguk is hozzájárulnak a világháló tudáshalmazainak – (multi)kultúrájának – együttes gyarapításához. A világháló nem jöhetett volna létre és nem is maradhatna fenn, ha az uralkodó közgazdasági paradigma szerint elválasztanánk egymástól például a vállalkozót és a fogyasztót, a szolgáltatót és a (ki)szolgáltatottat. Az internet nem *pay-per-view* tévékészülék, a virtuális tér közössége nem *pay-per-use* társadalom. Ebben a térben ugyanis a szimbolikus javak, a tudás, a kultúra elõállítása, cseréje és értelmezése folyik. Egy olyan jószág elõállításáé és cseréjéé, amelyre nem érvényesek a földi közgazdaságtannak a szûkösség elvére épülõ szabályai, mert minél szabadabban lehet hozzáférni ehhez a jószághoz, annál gyorsabban gyarapodik és annál nagyobb hasznot generál mindenki számára. Ennek a tudásnak a közege a hypertext vagy hypermédia, amely multilineáris, többirányú ösvény, tetszõlegesen választott csomópontokkal és kapcsolódásokkal rendelkezik, s a használó mint társalkotó ebben a közegben hozza létre a tudás változatos alakzatait. Ugyanígy nem lehet itt a használókat-létrehozókat földi származásuk és jogalanyiságuk különbözõségei szerint kategorizálni; a kibertérben a szabadság fokának meghatározásánál nem a legkisebb – amit például még a magyar és a kínai kormány is megengedne polgárainak, vagy a bahreini szultán alattvalóinak –, hanem a legnagyobb közös többszörös elve érvényesül.

Kibertér mint piactér

Amikor 1989–1990-ben Tim Berners-Lee és Robert Cailliau megalkotta a tudás hypertext alapú disztributív rendszerét, a World Wide Webet, és ezzel lehetõvé vált az adatok és információk online cseréje a genfi CERN és a bataviai (Illinois) Fermilab fizikusai között, majd 1993 novemberében megjelent a Mosaic és nyomában a többi felhasználóbarát böngészõ, hirtelen feltárulkoztak az eleddig néhány százezer ember közös ügyének planetáris méretû körvonalai. 1994-ben 18 millió, 1997-ben 90–100 millió, 1998-ban pedig már 150 millió használó írta és alkalmazta a világháló mûködésének szabályait. Becslések szerint 2001 augusztusában mintegy 514 millió ember használja az internetet az alapítók és az elsõ használók közössége által lefektetett szabályok szerint, amelyek tehát egyre nagyobb és szélesebb kör konszenzusára épülnek.[1] E rendkívül bonyolult globális rendszer zavartalan mûködése nyomán nap mint nap megtapasztalhatjuk azt, hogy a világhálót mûködtetõ szabályok jobbak, méltányosabbak, és nem utolsósorban hatékonyabbak, mint földi hasonmásaik. Nyilvánvaló, hogy e szabályok a világháló mûködése, növekedése során folyamatosan változnak, de a változások nem érintik létrehozásuknak a használók aktív részvételén és konszenzusán nyugvó alapelveit. Számos ígéretesnek indult, ám idõközben elvetélt vagy fejlõdésében megrekedt kommunikációs rendszer létrehozásának kísérlete bizonyítja, hogy létrehozóik sem technikai, sem közgazdasági, sem politikai értelemben nem értették meg a világháló és a hozzá hasonló globális rendszerek mûködtetésének emberi feltételeit. Ezért ha a világhálót magánvállalkozásként, a mikroökonómiai tankönyvekben lefektetett üz-

1 *Nua Internet Surveys,* 2001. http://www.nua.net/surveys/how_many_online/

leti szabályok szerint próbálták volna megvalósítani és mûködtetni – ahol a vállalkozó piacot kutat, befektet, információt állít elõ és árul, a fogyasztó pedig fizet és fogyaszt –, akkor az ma sem léphetett volna túl a France Télécom Miniteljének vagy a British Telecom Presteljének a szintjén. Röviden: a világháló lényegi vonásai közé tartozik, hogy a használat és a létrehozás, a szabályalkotás és a szabálykövetés nem különül el határozottan egymástól, s úgy tûnik, hogy ez a globális és dinamikus rendszerek mûködésének nélkülözhetetlen emberi feltétele.

Az internet gyorsuló fejlõdésével és terjedésével együtt és egyre határozottabban jelennek meg azok a politikai szándékok, amelyek az eleddig „leszabályozatlan" területet az állam által megszabott politikai-jogi keretek közé kívánják szorítani. S miután e fejlõdés következtében egy planetáris méretû üzleti vállalkozás lehetõségei immár kézzelfogható közelségbe kerültek, egyre határozottabban fogalmazódnak meg azok a gazdasági szándékok is, amelyek a kiszámítható, biztos és hatalmas hasznot ígérõ üzletmenet érdekében a világhálót „konszolidálni" akarják. Ezek a politikai és gazdasági szándékok nyilvánvalóan együtt járnak a digitális kultúra avantgárd utópiáinak visszanyesegetésével és kioltásával. Ezért, még ha a különféle kormányzati és üzleti tervezetek szerzõi át is veszik az internet elsõ, nonkonformista használóinak és teoretikusainak eredeti nyelvezetét, igyekeznek versenyre kelni velük új szavak, anagrammák és betûszavak kiötlésében, s a ma már szinte kötelezõ frázisgyûjtemény mögött gyakran tetten érhetõk a politikai ellenõrzés és korlátozás, a monopolizálás, a tartalom feletti kizárólagos rendelkezési jogok megszerzésének és hosszú távú biztosításának a kísérletei.

Az ellenõrzésre és a korlátozásra irányuló politikai és gazdasági szabályozási szándékok azonban már rövid távon is bizonyítják alkalmatlanságukat. Mindenekelõtt azért, mert gazdaságilag, politikailag és jogilag meg akarják osztani a kibertérben oszthatatlan használó-létrehozó és szabályalkotó-szabálykövetõ személyt, s mert figyelmen kívül hagyják e bonyolult és összetett globális rendszer mûködésének participáción és konszenzuson nyugvó alapelveit. A kívülrõl diktált szabályok nyomában azonnal megmutatkoznak a világháló mûködésének és további fejlõdésének korlátai, mert gátolják a tudás szabad áramlását és egyenlõ disztribúcióját, a használó-létrehozó személyek szabad kommunikációját. Amikor Steve Woolgar, a neves angol tudományfilozófus és az általa vezetett kutatócsoport tagjai elõször vetették fel írásaikban – lásd pl. „They came, they surfed, they went back to the beach", és „Virtual Society? Beyond the Hype" – az egykori használók fogalmát, sokan ezt még tökéletes õrültségnek tartották. Egyes becslések szerint azonban

2 Nincsenek megbízható módszerek az internethasználók számának pontos és megbízható mérésére, ezért az említett számot is sokan vitatják. Az internethasználók számának csökkenésére vagy növekedésére lehet következtetni például a kapcsolódás várakozási idejének mérésével is. Az átlagos várakozási idõ az Egyesült Államokban a 2000. õszi 20 másodpercrõl decemberre 16,3 másodpercre csökkent. Ezeket a mérési adatokat azonban nemcsak a használók száma, hanem az alkalmazott technikák és technológiák, illetve azok változásai is nagymértékben befolyásolják. Ugyanakkor az utóbbi idõben az adatforgalom növekedésérõl a korábbiakhoz képest sokkal reálisabb becslések jelentek meg (lásd ehhez Coffman és Odlyzko 2001). Az európai adatok vegyes képet mutatnak. Nyugat-Európában és a Balti államokban az utóbbi két évben folytatódott az internethasználók számának dinamikus növekedése, Magyarországon viszont 2000-ben lassulni látszott a korábbi növekedés üteme; elmaradásunk

mintegy 30 millióra tehetõ azon egykori használók száma, akik 1999-ben kiszálltak a virtuális térbõl.[2] A virtuális tér menekültjeinek elhatározását, paradox módon, nem a technikával szembeni fóbiájuk, nem a rousseau-i „vissza a természethez" érzése motiválta, s nem is Thoreau *Walden*jének partján akartak újra magányosan elmélkedni. A világháló elhagyásának egyik legfõbb okát a kibertér egyre növekvõ kommercializációjában jelölték meg. A kommercializáció következtében üzleti ajánlatok és információk (ígéretek) olyan tömege zúdul a használóra, amelyekre egyáltalán nincs szüksége, idejét és pénzét emészti, a szoftverekben elrejtett kémprogramok (spyware, executable applets vagy cookies, adbots, browser parasites, web bugs stb.) pedig számítógépén tárolt adatai és használói szokásai után kémkednek, kereskednek azokkal tudta és beleegyezése nélkül. Az így vándorútra kelõ személyes adatok nyomában üzleti ajánlatok és haszontalan információk újabb áradata zúdul a használóra. Serge Gauthronet és Etienne Drouard becslése szerint az elektronikuslevél-marketing (spamming) 2000-ben mindegy 10 milliárd euróval növelte a használók éves internetköltségeit. A szerzõk a használókat terhelõ reklámköltségek mellett egy súlyosabb veszélyre is felhívják figyelmünket: a spammingvállalkozások ma már naponta akár 20 milliárd levél elindítására is képesek, s ez az „entrópia jelenségének rémét" szabadíthatja rá a világhálóra.[3] Az e-gazdaságnak ebben a fontos, üzlet- és fogyasztó- (B2C) szegmensében a virtuális tér használó-létrehozó személye kellemetlenebb és kiszolgáltatottabb helyzetbe kerülhet, mint a földi gazdaság egyszerû fogyasztójáé. Ezt a tendenciát támasztja alá pl. az Amazon.com 2000. augusztus 31-i közleménye is: eszerint a vállalkozás saját vagyontárgyának *(private assets)* tekinti 20 millió ügyfele személyes adatait, amelyeket ezentúl szabadon és üzleti érdekeinek megfelelõen szándékozik hasznosíta-

---

(2. folyt.) szembetûnõ Ausztriához, de Szlovákiához és Szlovéniához képest is, az okok nincsenek alaposan feltárva. Minden bizonnyal a Matáv tarifapolitikája és távközlési monopóliuma, a digitális kultúra oktatásának periferikus volta, és ennek következtében a magyar tartalomszolgáltatások fejlõdésének lassúsága is szerepet játszhat. E feltételek megváltoztatása nélkül talán nem is növelhetõ lényegesen az internetezõk száma. Mert a 650 000 magyar használó népességbeli aránya közel eshet ahhoz a felsõ társadalmi határhoz, amelynek tagjai meg tudják fizetni az internetezés magas hazai költségeit, és rendelkeznek azzal a kulturális tõkével (nyelvi, technikai és szakmai tudással), amely lehetõvé teszi számukra, hogy „potyautasként" is élni tudjanak a világháló kínálta gazdasági és kulturális lehetõségekkel. Az *eMarketer* elemzõje, Nevin Cohen kedvezõbb képet fest a magyarországi helyzetrõl, s magasabb számokat közöl a digitális kultúra elterjedtségérõl és kilátásairól. Adatai szerint 2000 októberében 715 000 magyar internethasználót mértek. S a *Carnation Research* kutatására hivatkozva, 2001 végére szerinte 969 000 magyar használója lesz a világhálónak. Ezek a számok azonban mit sem változtatnak azon a tényen, hogy a magyar internethasználók számának növekedése jelentõsen elmarad az említett környezõ országokétól (Nevin Cohen: „Hungary's Healthy eOutlook", 2001. február 13. http://www.emarketer.com/analysis/eeurope/20010213_europe.html; *Nua Internet Surveys, 2000* http://www.nua.net/surveys/how_many_online/europe.html; European Survey of Information Society Knowledge Base http://europa.eu.int/ISPO/esis/default.htm; *Measuring Information Society 98* http://europa.eu.int/ISPO/polls/98/poll98/index.htm).

3 (Gauthronet és Drouard 2001: 71–74). Az Európai Bizottság számos dokumentumában – lásd pl. Directive 97/7/EC, Directive 97/66/EC és Directive 2000/31/EC – szûrõprogramokat javasol a spamming ellen. Nem igazán hatásos eszközök. Az Egyesült Államokban a szolgáltatók igyekeznek blokkolni azokat a szervereket, amelyek spamlevelek tömegét indítják el. Újabban az Európa Parlament a **cookie** használatának általános tilalmát tervezi (Matt 2001; Stephens 2001).

ni. Röviden, az Amazon.com annak adja el húszmillió vásárlója személyes adatait – nevét, címét, telefonszámát, e-mail-címét, a hitelkártyájáról és pénzügyeirõl, iskolai végzettségérõl, foglalkozásáról és munkahelyérõl szerzett információkat, társadalombiztosítás-számát, jogosítványának adatait stb. –, aki azokért a legtöbbet kínálja.[4]

Az Európai Tanács megbízásából készült, 1994 májusában kiadott *Bangemann Report* a vállalati marketing stílusában piacvezérelt forradalomként írja le a globális információs társadalom kialakulásának folyamatát. A jelentés készítõiben fel sem merült annak a lehetõsége, hogy éppen a piaci vezérlés kiteljesedése állítja majd a legnagyobb akadályt a piac korlátlan bõvíthetõsége és az információs társadalom kialakulása elé. Az információs társadalom másfajta technikai, gazdaságelméleti, jogi és politikai gondolkodást igényelne. Máskülönben az egyre agresszívebb kommercializáció, a használóra kényszerített haszontalan információk áradata, személyes adatainak és szokásainak illetéktelen, üzleti és egyéb célú felhasználása, a tudáshalmazok feletti gazdasági ellenõrzés megszerzése és monopolizálása magát az embert fogja kiszorítani a virtuális térbõl. Mindenestre úgy tûnik, a kibertérben megvalósulni látszanak Robert Rocherfort korábbi megállapításai, amelyeket az 1990-es évek fogyasztói szokásainak változásairól és azok társadalmi következményeirõl tett. Rocherfort szerint a fogyasztó számára azért vált rendkívül körmönfonttá a játék ebben az új gazdasági környezetben, mert egyszerre próbál hasznot húzni a piac személyesen neki címzett ajánlataiból, s ugyanakkor piacmentes övezetté szeretné tenni saját privát szféráját. A két törekvés közötti határ azonban igen tünékeny; az új igények és szükségletek sikeres kommercializálása jelzi e határnak a privát szféra hátrányára történõ áthelyezését (Herzlich és Vaysse 1993).

Jog és politika a kibertérben

Az internethasználat növekvõ népszerûségével és elterjedtségével egy idõben jelentek meg az államok egyre határozottabb szabályozási törekvései, amelyek többnyire nem a használó-létrehozó személy kiberjogainak védelmére, hanem sokkal

4 Az itt felsorolt személyes adatok listája az Amazon.com *Privacy Notice* címû dokumentumából származik. Az Amazon.com itt ajánlásokat is megfogalmaz azon vásárlók számára, akik ezt az adatgyûjtést és adatkereskedelmet elfogadhatatlannak tartják, õk kénytelenek úgynevezett titoktársaságokon *(Privacy Companies)* keresztül elküldeni megrendeléseiket. A titoktársaságok egyébként évi 49,99–229,99 USD-t számolnak fel szolgáltatásaikért; az évi 49,99 USD elõfizetés pusztán az anonim barangolást teszi lehetõvé. A Privacy International és az Amazon.com.uk levelezése azt mutatja, hogy az Amazon.com.uk nem óhajtja megérteni a Privacy International képviselõinek a személyes adatok tárolására és ellenõrizetlen transzferére vonatkozó kifogásait. Az Amazon.com.uk képviselõje elég sajátosan érvel a személyes adatok tárolása mellett; vásárlóik hitelkártyájának adatait például azért nem törlik, mert az nagyon idõigényes (lásd http://www.privacyinternational.org/issues/compliance/amazon).

Ugyanakkor egyre több úgynevezett freeware-t ajánló vállalkozás (BearShare, GoZilla, Speedbit, Acoustic Galaxy, Radiate/Aureate stb.) gyûjti a programjaiba elhelyezett spyware-ek révén személyes adatainkat, és folyamatosan ellenõrzi felhasználói szokásainkat. E vállalkozások eredeti szándékairól sokat elárulnak maguk az agresszív programok, amelyek a telepítés után a kevésbé gyakorlott felhasználók számára szinte kiirthatatlanok a számítógéprõl.

inkább azok korlátozására, a kommunikáció szabadságának szûkítésére, a tudáshalmazok ellenõrzésére és elõzetes cenzúrázására irányultak. Ezért bárhogy is vélekedjünk a digitális kultúráról és a világháló mûködésének libertinus politikai filozófiai alapelveirõl, világosan kell látnunk azt, hogy a világháló szabályozására és ellenõrzésére irányuló politikai és gazdasági törekvésekkel szembeni ellenállás és tiltakozás nemcsak kiberjogaink biztosításának, hanem számos esetben nehezen megszerzett földi jogaink védelmének érdekében is történik. Az Egyesült Államok, az Európai Unió és az egyes tagállamok, valamint az Európa Tanács eddigi törvényhozási kezdeményezései szûkítik, korlátozzák, vagy egyenesen visszavonják azon emberi jogok és alapvetõ szabadságok némelyikét a virtuális térben, amelyeket például az amerikai alkotmány elsõ és negyedik kiegészítése, az Emberi Jogok Egyetemes Nyilatkozata, az Emberi Jogok és Alapvetõ Szabadságjogok Európai Egyezménye, az egyes országok alkotmányai és törvényei a földi halandók számára egyszer már biztosítottak. Nagy-Britannia, Németország, az Európai Unió vagy az Európa Tanács törvénytervezetei és ajánlásai ellentétesek az emberi jogok és alapvetõ szabadságok védelmérõl szóló római egyezménynek a véleménynyilvánítás szabadságáról, a levéltitokról és a jogorvoslathoz való jogról szóló cikkeivel, valamint a strasbourgi emberi jogi bíróság joggyakorlatával és döntéseivel.[5] Ráadásul gyakran kriminalizálnak és szankcionálni szándékoznak olyan nem szándékos és másoknak hátrányt vagy sérelmet nem okozó cselekedeteket – például elektro-

5 Az *Emberi Jogok és Alapvetõ Szabadságjogok Európai Egyezménye* art. 6. és 8. megsértése miatt számos ügy került a strasbourgi bíróság elé, amelyekben a bíróság az államokat marasztalta el. Lásd ehhez például Funke v. France (1993), John Murray v. the United Kingdom (1996), Saunders v. the United Kingdom (1996), Serves v. France (1997), illetve Malone case (1983), Halford v. the United Kingdom (1997), Huvig case (1989), Kruslin case (1989), Niemietz v. Germany (1991), Amann v. Switzerland (1995), Kopp v. Switzerland (1997) és Valenzuela Contreras v. Spain (1997).

6 Nagy-Britanniában az *Investigatory Powers Act* (2000) art. 53 (1) és (5) a titkosító kulcs hatóságok elõtti eltitkolását két évig terjedõ börtönbüntetéssel szankcionálja. A törvény célja elég nyilvánvaló, tudniillik megakadályozni a gyanúsított ama szándékát, hogy kriminális cselekedeteinek dokumentumait, levelezését hozzáférhetetlenné tegye a hatóságok számára. De ha a hatóságok a titkosított dokumentumokkal akarják megalapozni a gyanúsítottal szembeni vádat, akkor minek az alapján gyanúsították? Senki sem kényszeríthetõ arra, hogy önmagát vádolja. Mint ahogy ártatlanságának bizonyítására sem. Ezért a törvény alapvetõen sérti az *Emberi Jogok és Alapvetõ Szabadságjogok Európai Egyezmény*ének 6. artikulusát. Ugyanakkor a törvény egyéb következményeit tekintve is ellentmondásos, mert nem tud és nem is akar világos különbséget tenni a titkosító kulcs átadásának szándékos megtagadása, korábbi szándékos törlése vagy véletlenszerû elvesztése között. Ez pedig a hatóságok önkényes értelmezése elõtt nyitja meg az utat a személy szándékait illetõen, vagyis kriminális cselekedeteit leplezendõ tagadja meg a kulcs átadását, következésképpen bûnös. Bevallom, hogy én már kétszer vesztettem el leveleim titkosító kulcsát, ráadásul egy új biztonsági program kipróbálása során tévedésbõl a sajátom helyett éppen egy angol barátom levelezõprogramját láttam el titkosító kódommal. Miután nagy nehezen sikerült visszaállítani az eredeti állapotot, eldobtam persze ezt a kulcsot is. Igaz, ez utóbbi esetben nem én, hanem õ lenne büntethetõ (Bowden 1999; Akdeniz és Bowden 1999: 81–125).

Kevésbé szigorú, de nem kevésbé megalapozatlan az ír *Electronic Commerce Act* (2000) art. 27 (4)-e. Eszerint kihágást („summary offence") követ el az, aki a hatóságok elõtt megtagadja titkosított üzenetének dekódolását. Ezzel szemben a belga *Loi du 28 novembre 2000 relative à la criminalité informatique* art. 88. quater. § 1–3. viszont a gyanúsítottat nem, csak harmadik személyt kötelezne a titkosító kulcsok átadására. Ennek megtagadását pedig 6–12 hónap börtönbüntetéssel és/vagy 26–200 ezer

nikus levelezésünk titkosító kulcsának a törlését, elvesztését vagy átadásának szándékos megtagadását Nagy-Britanniában és Írországban –, amelyeken a földi térben egyáltalán nem ütköznénk meg.[6] Az utóbbi két évben ezekhez a jogokat és szabadságokat különbözõ mértékben szûkítõ, megszorító törvényhozási kezdeményezésekhez zárkózott fel többek között Kína, Ausztrália, Új-Zéland, India, Dél-Korea, Japán, Szingapúr, Malajzia és Törökország (Anderson 2001; Bingham 2001; Le CSA veut contr ler les images et les sons du Net. In Vnunet.fr, 2001. máj. 31.; Dearne 2001; Kim Deok-hyun 2001; Ko Shu-ling 2001; Latrive 2001; Lal Pai 2001; Taggart 2001). A nyilvános hazai kormányzati dokumentumokból nem lehet arra következtetni, hogy Magyarország is ehhez a trendhez készülne igazodni, legfeljebb egyes kormánytisztviselõk és politikusok nyilatkozatai utalhatnak erre.[7] Az Európa Tanács számára a május 25-én elkészült legújabb ajánlás – a *Convention on Cyber-crime* (2001) –, amelyhez a tervek szerint 2001. november 23-ától csatlakozhatnak az egyes tagállamok, többek között éppen az emberi jogok és szabadságok korlátozása miatt került a kiberjogi, az emberi jogi és a különféle informatikai szakmai szervezetek bírálatának középpontjába. A heves és széles körû nemzetközi tiltakozás ellenére a tervezet készítõi úgy vélik, hogy munkájuk hozzá fog járulni a kibertér új nemzetközi jogrendjének kialakításához.[8] Meglehet. De ez eléggé valószínûtlen egy olyan nemzetközi jogi dokumentum esetében, amely a legteljesebb homályban hagyja az államok szuverenitásának és autoritásának kérdését, amely nem akar tudomást venni a nem lokalitás elvérõl, ellentmondásosan veti fel

---

(6. folyt.) belga frank pénzbüntetéssel szankcionálná. Az említett európai országokon kívül Szingapúr és Malajzia alkotott törvényt a jelszó vagy titkosító kulcs átadásának kötelezettségérõl. Az Európa Tanács *Convention on Cyber-crime* (2000) tervezete viszont ebben a vonatkozásban folyamatosan változott, s a végleges dokumentumban (a 27. változatban) már nem esik szó sem errõl, sem a key-eschrow rendszerrõl.

7 Ez a törekvés a magyar kormányzati dokumentumokból – *Magyar válasz* (1999) és *Tézisek az információs társadalomról* (2000) – nem olvasható ki még akkor sem, ha politikusi nyilatkozatokban és írásokban olykor megfogalmazódik a világhálót jellemzõ kommunikációs szabadsággal szembeni nyugtalanság, s a kontroll bevezetésének szükségessége (lásd Rockenbauer és Újvári 2001; Körmendy-Ékes 2000). Ugyanakkor néhány, a kommunikáció ellenõrzésére, a tartalmak elõzetes cenzúrázására magánszorgalomból tett lépés alapján arra lehet következtetni, hogy egyes szolgáltatók és szervezetek tévesen definiálják saját helyüket, szerepüket és jogosítványaikat ebben a nyilvános kommunikatív térben (lásd ehhez Bogád 2001).

8 Lásd Csonka Péternek, az Európa Tanács Gazdasági Bûnözés Kollégiuma helyettes vezetõjének nyilatkozatát (Luening 2000). Ezzel szemben számos szakértõ úgy látja, hogy a tervezet alapvetõ ellentmondásai miatt „teljes kudarccal végzõdhet" az alkalmazás során (*BDRC Report on Safer Internet Action Plan: Intermediate Evaluation, Conducted for the European Commission*, Vol. 2. 2001. máj. 31., 7–8.).

Az EPIC és több nemzetközi civil szervezet azt is kifogásolja, hogy az amerikai kormányzat segítségével készült tervezet az amerikai joggal összhangban kriminalizál olyan magatartásokat, amelyek az Egyesült Államokon kívül nem kriminalizálnak, vagy az európai országokban enyhébb megítélés alá esnek (McCullagh 2000). A *Convention on Cyber-crime* (2000) egyik kiemelt feladata a gyûlöletbeszéd visszaszorítása és üldözése lenne a kibertérben. Ahogy azonban a náci relikviákat kaliforniai honlapján árverezõ Yahoo! International Inc. és a La ligue contre le racisme et l'antisemitisme közötti perben 2001. november 7-én hozott kaliforniai bírósági ítélet bizonyítja, ez nem valósítható meg az

a büntetõjogi felelõsség kérdését, pontatlanul és kiterjesztõ módon határozza meg a számítógép- és kiberbûnözés fogalmát, és totális, minden adatra és minden egyes személy adatforgalmára kiterjedõ ellenõrzéssel kívánja üldözni a kiberbûnözést a virtuális térben.[9] A francia kormány részére 1996-ban készült dokumentum, az *Internet, Enjeux juridique* szerzõi még az „a priori korlátozás helyett az önkorlátozást" javasolták a kormányzatnak.[10] Egy másik kormányzati dokumentum írói – *La France dans la société de l'information* (1999) – hasonló szellemben fogalmazták meg a szabályozást, az államok szuverenitását, az e szuverenitás határait és a világháló határtalanságát érintõ politikai és jogi dilemmákat: „Az internet kollektív alkotás, mindig befejezetlen, változó szabályainak gyakran csak akkor van értelmük, ha azokat az egész világon alkalmazzák. Ha az államok nem akarnak lemondani hivatásukról és felelõsségükrõl, akkor meg kell találniuk az internet magán- és közösségi, technikai és üzleti szereplõivel a dialógus új módozatait."[11] Úgy tûnik azonban, hogy az államok még nem találták meg, s nem is nagyon keresik ezeket az új módozatokat. A politikai gyakorlat és a törvényhozási kezdeményezések sokszor ellentmondanak azoknak az emelkedett stílusban megfogalmazott nagyszabású hivatalos utópiáknak, amelyeket az egyes kormányzatok az információs vagy kommunikációs társadalom jövõjérõl fogalmaznak meg.

Mielõtt részletesen elemeznék néhány olyan törvényt, továbbá nemzetközi és kormányzati kezdeményezést, amely a világhálón zajló kommunikáció és e kommunikáció tartalmainak a szabályozását tûzte célul, elõzetesen rá kell mutatni arra, hogy e kísérletek haszontalannak és eredménytelennek bizonyultak, mert nem tudták elérni kitûzött céljaikat, ráadásul emberi jogokat és alapvetõ szabadságokat sértettek. Hatásuk sokkal inkább abban mutatkozott meg, hogy felbosszantották és mozgósították a világhálót használó-létrehozó személyek és szervezetek sokaságát, akik ezután különbözõ alkotmánybírósági és legfelsõbb bírósági döntések nyomán sikeresen szerezték vissza az új törvények által korlátozott vagy kétségbevont jogaikat. Úgy tûnik, hogy az alkotmánybírák – a törvényhozókkal ellentétben – nem te-

---

egyes országok alkotmányainak és joggyakorlatának különbségei miatt.

9 Az utóbbi években az Európa Tanács a személyes adatok védelmérõl számos ajánlást fogalmazott meg. Így például a *Recommendation No R (99) 5* rámutat a személyes adatok folyamatos gépi gyûjtésének és rögzítésének veszélyeire és törvénytelenségére, s arra ösztönzi a használókat, hogy személyes adataikat leghatásosabban anonimitásuk megõrzésével, leveleik titkosításával, illetve a felelõtlen szolgáltatók bojkottálásával védhetik meg (lásd például Council of Europe, *Recommendation No R (99) 5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet,* 1999. február 23.; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* [ETS No 108] Strasbourg, 1981. január 28.). S ugyanígy a tervezet nem tesz világos különbséget a computer-related és a computer-mediated crime között; az elõbbi kategória alá sorol olyan cselekményeket, amelyek a földi térben történnek. Így nem csoda, hogy a tervezetben a számítógép-kultúra mint valami posztmodern infernó jelenik meg (lásd ehhez MacKinnon 1997: 209–211).

10 Internet, Enjeux juridique: Rapport au ministre délégué à la Poste aux Télécommunications et à l'Espace et au ministre de la Culture, Présidée par Isabelle Falque-Pierrotin. 1996. márc. 16.–jún. 16., 9–10.

11 La France dans la société de l'information. Paris, 1999. 18.

12 American Civil Liberties Union v. Reno 117 S. Ct. 2329 (1997); American Library Association

kintik a világhálót alkotmánymentes övezetnek.[12] Számos esetben hosszú és fáradságos jogi procedúrákra sem volt szükség, mert ezek nélkül is megbuktak a világhálót használó-létrehozó személyek ellenállásán. A világhálót szabályozni kívánó törvények feletti viták során gyakran vádolták az amerikai, a német, az angol törvényhozókat vagy a brüsszeli bizottság tagjait azzal, hogy nem ismerik a globális rendszer mûködésének alapelveit, és nem értik a világháló valódi problémáit. Ez persze nem teljesen alaptalan feltételezés. (Igaz, a legfontosabb kérdésekben – hogyan változtatja meg a világháló a társadalmi kommunikáció hagyományos formáit és normáit, átalakítja-e a kommunikáció köz- és személyes tereit, miként hozza létre a tudás változatos alakzatait, milyen hatása van az írásra és általában a nyelvre, s mindezeknek milyen társadalmi, gazdasági, politikai és kulturális következményei lehetnek a jövõ társadalmában? – mindannyian tudatlanok vagyunk.) Patrick Leahy, Vermont demokratapárti szenátora a *Communications Decency Act* (1996) szenátusi vitája során maga is utalt arra, hogy a száz szenátor közül eleddig csupán hatan használták az internetet.[13] Ezért fogalmazott találóan Louis Rossetto, a *Wired* szerkesztõje az említett törvény elleni tiltakozó felhívásában: A törvény olyan, „mint amikor írástudatlanok mondják meg nekünk, hogy mit olvassunk. A Kapitóliumban a politikusok kisebbsége rendelkezik csak e-maillel, s a kongresszus sincs teljesen rákapcsolva az internetre".[14] Az emberi jogok szûkítése mellett ugyancsak a hozzáértés hiánya miatt bírálják adatvédelmi, informatikai és biztonsági szakemberek az Európa Tanács *Convention on Cyber-crime* (2001) tervezetét. A tervezet ugyanis akadályokat állít azon technikák és szoftverek alkalmazása és fejlesztése elé, amelyek éppen a számítógépek és a számítógép-hálózatok biztonságát, az adatok védelmét, az adatforgalom hitelességét és az üzleti tranzakciók megbízhatóságát kívánják szolgálni külsõ, illetéktelen behatolókkal szemben.

---

v. Pataki 969 F. Supp. 160 (S.D.N.Y. 1997).

13 Bõvebben Statement of Senator Leahy On Introduction of The Child Protection, User Empowerment, and Free. *Expression In Interactive Media Study Bill,* 1995. április 7. http://leahy.senate.gov/press/ 199507/950721.html és *The Role of DOJ and Internet Protest*, 1995. december 14. http://leahy.senate.gov/ press/199512/951214.html.

14 Rossetto felhívásának lelõhelye: http://hotwired.lycos.com/special/indecent/louis.html. Természetesen Leahy és Rosetto kijelentései az 1995-ös állapotra vonatkoznak.

A magyar Országgyûlés informatikai helyzetét és a képviselõk tájékozottságát jól jellemzi Zuschlag János szocialista képviselõ önálló határozati javaslatának fogadtatása. A képviselõ azt kérte az Országgyûléstõl, az utasítsa hivatalát arra, hogy „mindennemû, a képviselõi munkához kapcsolódó információt digitalizáljon, számítógépes programokkal olvasható, feldolgozható formátumban is tegye hozzáférhetõvé a képviselõk számára, a papírdokumentumokkal azonos idõben". Jóllehet a képviselõk rokonszenveztek Zuschlag javaslatával, mégis futurisztikus és elhamarkodott elképzelésnek igyekeztek azt beállítani. A képviselõ javaslata meglehetõsen visszafogottnak tûnik annak ismeretében, hogy az Európa Parlament és a nyugat-európai országok parlamentjeinek dokumentumai szabadon hozzáférhetõk az interneten. A törvényhozó és a kormányzati munka átláthatóságának megteremtését a nyugat-európai kormányok kiemelt feladatként kezelik. Lásd például a francia *Service d'information du Gouvernement* (SIG) http://www.internet.gouv.fr; az angol *White Paper on Modernizing Government,* March 1999, és a *European Governments on-line* http://europa.eu.int/abc/governments/index_en.html. Mindenesetre ez az elvetélt javaslat is pontosan mutatja, hogy milyen mély kulturális, tudásbeli és technikai szakadék húzódik a világháló magyar használói és a világháló használatáról

Ráadásul a tervezet az ügyfelek tranzakcióinak és adatforgalmának folyamatos rögzítésére és archiválására kötelezi az internetszolgáltatókat (ISP); a totális ellenõrzés következtében létrejövõ, a magánszemélyek, szervezetek és vállalkozások tevékenységének minden részletét és egész történetét felölelõ hatalmas adatbázisok pedig könnyen válhatnak illetéktelen behatolók szabad prédájává.[15]

A tökéletesen ellenõrzött társadalom felé

Az Európa Tanács *Convention on Cyber-crime* (2001) tervezete jól példázza azt a kétértelmûséget, ahogyan a törvényekben és a törvénytervezetek íróinak képzeletében a világhálót mûködtetõ technikák és technológiák megjelennek. A tervezet készítõi hisznek abban, hogy a technika kezükbe adja az állami ellenõrzés fegyverét, ugyanakkor félnek attól, hogy ki is üti a kezükbõl ezt a fegyvert. A technika fejlesztésével és fejlesztésének korlátozásával akarják megvalósítani a virtuális tér totális ellenõrzését; ezért egyfelõl bizonyos technikák létrehozásának és alkalmazásának monopolizálására, másfelõl ugyanezen technikák létrehozásának és alkalmazásának korlátozására, tiltására és kriminalizálására törekszenek. Az Európa Tanács tervezetének legfõbb kezdeményezõi, a nyugat-európai országok számtalanszor kinyilvánították, hogy mennyire fontos számukra az adatok hitelességének és integritásának a védelme, az adatforgalom biztonsága és a személyes adataink

---

majd törvényeket alkotni kívánó magyar Országgyûlés között (*Origo*, Hírek, 2001. február 5., hétfõ, 15.57).

15 *Convention on Cyber-crime* (2001) art. 17–18., 20–21. (Draft Nº 27, REV. 2). Az idézett helyek alapvetõen ellentétesek az OECD *Recommendation of the Council Concerning Guidelines for Cryptography Policy, 27 March 1997* címû dokumentumában megfogalmazott ajánlásokkal. Az OECD-ajánlás többek között az adatok megbízhatóságának, integritásának és elérhetõségének a fontosságát hangsúlyozza, s a kriptográfiát az információs technológiák biztonságos használatának hatékony eszközeként tárgyalja. A következõképpen fogalmaz: „Felismerve azt, hogy a kriptográfiai módszerek alkalmazásának hiánya ellentétes hatással van a magánélet, a szellemi javak, az üzleti és a pénzügyi információk, a köz- és nemzetbiztonság védelme és az elektronikus kereskedelem mûködésére – mert ha az adatokat és a kommunikációt nem védelmezzük meg az engedély nélküli hozzáféréssel, a megváltoztatással és az illetéktelen használattal szemben, a használók nem fognak megbízni az információs és kommunikációs rendszerekben, hálózatokban és infrastruktúrákban."

Ulrich Sieber az Európai Unió részére készített ajánlásában láthatólag nem érzékeli a probléma lényegét. Szerinte „… a számítógépek közötti telekommunikáció nem szolgál rá nagyobb védelemre, mint a személyek közötti". A konfliktus azonban éppen abból ered, hogy az államok nem akarják elismerni a személyek közötti kommunikációra vonatkozó alkotmányos jogok érvényességét a számítógépek által közvetített kommunikáció esetében (Sieber 1998: 116; lásd még *Common Position on data protection aspects in the Draft Convention on Cyber-crime of the Council of Europe,* adopted by International Working Group on Data Protection in Telecommunications at the 28th meeting of the Working Group on 13./14. Berlin, 2000. szeptember).

16 A folyamatos és korlátlan adatgyûjtés veszélyét jelzi a svájci *Sonntags Zeitung* 2001. február 4-i híre, mely szerint hackerek törtek be a davosi Világgazdasági Fórum szerverére, és megszerezték 1400 vendég, többek között Bill Clinton, Bill Gates, Yoshiro Mori és Jasszer Arafat személyes adatait (lakcímét, e-mail-címét, bankkártyaszámát, mobilszámát, útlevélszámát, internetes jelszavaikat stb.). A hackerek CD-n juttatták el az adatokat a szerkesztõség címére. Számos nemzetközi dokumentum – emberi jogi és biztonságtechnikai szempontból egyaránt – elfogadhatatlannak tartja az ilyen

titkosságához fûzõdõ emberi jog – a tervezet e deklarációk ellenére mégis kezdeményezi a személyek és szervezetek adatainak és adatfogalmának az internetszolgáltatókon keresztül történõ totális ellenõrzését.[16] A személy alapvetõ információs jogaira és az elektronikus gazdaság és kormányzás érdekeire vonatkozó állásfoglalások mellett az Európai Unió különféle bizottságainak és szervezeteinek hivatalos dokumentumaiból határozottan kiolvasható az a törekvés, hogy az államok – jobb megoldás híján – az internetszolgáltatókra kívánják hárítani a totális ellenõrzés technikai feltételeinek megteremtését és mûködtetését. Ennek érdekében az internetszolgáltatóknak olyan jogosítványokat terveznek adni és olyan kötelezettségeket kívánnak hárítani rájuk, amelyek egyáltalán nem vezethetõk le a szolgáltatók mint üzleti vagy nem profitérdekelt vállalkozások jogállásából, s az ügyfél és a szolgáltató – mint szabad, egyenrangú és mellérendelt felek – között fennálló szerzõdéses jogviszonyból. Ezek ellentétesek például a *Directive on Electronic Commerce* (2000) 15. cikkében megfogalmazott alapelvvel, amely szerint „A tagállamok nem róhatnak olyan általános kötelezettséget a szolgáltatókra, akik a 12., 13. és 14. cikk szerint végzik tevékenységüket, hogy ellenõrizzék az általuk továbbított vagy tárolt információkat, vagy aktívan nyomozzanak illegális tevékenységre utaló tények és körülmények után".[17] A *Convention on Cyber-crime* (2001) és hasonló tervezetek ugyanakkor alapvetõ kérdéseket hagynak megválaszolatlanul: felhatalmazhat-e vagy kötelezhet-e az állam üzleti vállalkozásokat tartalmak elõzetes cenzúrázására, felhatalmazhatja-e vagy kötelezheti-e azokat ügyfeleik kommunikációjának és adatforgalmának a rögzítésére, archiválására és átadására, kódolt adataik dekódolására és mindezen feladatok anyagi és technikai feltételeinek megteremtésére? Ilyen kötelezettségek egész sorát tartalmazza az Európai Unió Tanácsának 1995. január 17-i határozata, a *Resolution on the Lawful Interception of Telecommunications,* így például azt is, hogy bizonyos esetekben a szolgáltatók feladata lenne ügyfeleik kódolt üzeneteinek dekódolása.[18]

Ez utóbbi kötelezettség is jelzi azt, hogy az államok szabályozási törekvései elsõsorban azokra a technikákra és technológiákra vonatkoznak, amelyek a világháló biztonságos adatforgalmát, az adatok hitelességét és integritását, a számítógépeket és a használókat azonosító címek védelmét szolgálják. A Wassenaar Arrangement (1996) és annak két évvel késõbb elfogadott bécsi kiegészítése nyomán az

---

adatbázisok létrehozását, illetve az ilyen típusú adatok tárolását. (Thomas Isler–Oliver Zihlmann, „WEF-Gegner stahlen Geheimdaten der Mächtigen Hacker kopierten illegal Kreditkartennummern, Pass-, **(16. folyt.)** Handy- und Privatnummern von 1400 Wirtschaftsführern", *Sonntags Zeitung,* 2001. febr. 4. http://www.sonntagszeitung.ch. Lásd még Edouard Launet, „Piratage au sommet à Davos", *Libération*, Le vendredi 2 février 2001; Chris Gaither, „Digitalhackers Steal Data From Economic Forum", *New York Times*, February 6, 2001.)

17 *Directive 2000/31/EC* of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *Official Journal L 178 ,* 17/07/2000 p. 0001 – 0016.

18 Resolution of 17 January 1995 On the Lawful Interception of Telecommunications (96/C329/01), Official Journal of the European Communities, November 4, 1996. art 3.3. Vö. Recommendation 2/99 on the Respect of Privacy in the context of Interception of Telecommunications, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Brussels, 3 May 1999. és Recommendation 3/99 on the Preservation of Traffic Data by Internet Service Providers for Law

aláíró államok többsége bizonyos megszorításokkal ugyan, de lehetõvé tette a kriptográfiai szoftverek szabad kereskedelmét és alkalmazását, ugyanakkor egyes államok törvényei és törvénytervezetei különféle jogi eszközökkel és technikai elõírásokkal igyekeztek az általános könnyítések feltételezett negatív hatásait ellensúlyozni.[19] Úgy tûnik, hogy az államok nem tudják feloldani az információ és a kommunikáció szabadságának, az elektronikus gazdaság és kormányzás biztonságának megteremtése és az ellenõrzõ állam különleges jogosítványainak – „lawful access" – korlátlan gyakorlása közötti érdekellentéteket. Ezért az államok egészen az utóbbi idõkig azon biztonsági megoldások bevezetését részesítették elõnyben, amelyek valamilyen módon – Clipper Chippel, kriptográfia használatának hatósági engedélyeztetésével, titkosító kulcsok letétbe helyezésének kötelezettségével (key-escrow vagy key-recovery systems), erõs kriptográfiai kulcsok tiltásával, exportkorlátozással és hasonlókkal – szabad bejárást, úgynevezett „hátsó ajtót" hagytak volna személyek és szervezetek kommunikációjába és adataiba az állami ellenõrzés számára. Mindenekelõtt az Egyesült Államok, Franciaország, Fehéroroszország és Oroszország, valamint Kína, Pakisztán, India és Szingapúr ragaszkodik ezekhez az eszközökhöz, még akkor is, ha nyilvánvaló, hogy alkalmazásuk emberi jogokat sért, s ráadásul veszélyezteti a kommunikáció, az adatok és az adatforgalom, az elektronikus gazdaság biztonságát.[20] Ahogy a Global Liberty Internet Campaigne szervezõi a *Wassenaar Arrangement* bécsi titkárságának címzett tiltakozó levelükben fogalmaznak: „bármilyen kötelezettség, amely a titkosító kulcsok letétbe helyezésére (key-escrow or key-recovery systems) vonatkozik, a személyes kommunikációk törvénytelen lehallgatásának velejáró és szükségtelen kockázatát idézi elõ".[21] A világháló használói-létrehozói nem olyan információs vagy kommunikációs társadalomban szeretnének élni, amelyben az államnak szabad bejárása van az egyén személyes és üzleti kommunikációjába, valamint különbözõ szervereken vagy saját számítógépén tárolt adataiba. Ezért az eddig megszületett törvények és rendeletek, így például a kriptográfiai szoftverekre vonatkozó exportkorlátozás az Egyesült Államokban, vagy a titkosító kulcs hosszúságát meghatározó rendeletek sora Franciaországban, nem érték el eredeti céljaikat – a világháló használói jószerével teljesen figyelmen kívül hagyták õket.

Az Egyesült Államok számos kezdeményezése, így például a kriptográfiai szoftverekre vonatkozó exportkorlátozás, vagy a Clipper Chip-tervezet egyenesen ellentétes hatást váltott ki a kibertérben. A *Digital Telephony Bill* (1994) például arra kötelezte volna a szoftverek, számítógépek és kommunikációs berendezések amerikai gyártóit, hogy építsenek be ilyen „hátsó ajtót" termékeikbe a korlátlan állami (amerikai) ellenõrzés biztosítása érdekében. Az alkotmányos jogok megsér-

---

Enforcement Purposes, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Brussels, 7 September 1999.

19 Bert-Jaap Koops, *Crypto Law Survey* http://cwis.kub.nl/àfrw/people/koops/lawsurvy.htm; Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, Hague, 1999.

20 GILC, *Cryptography and Liberty: An International Survey of Encryption Policy*, Washington DC, February 1998. http://www.gilc.org/crypto/crypto-survey.html.

21 *GILC Statement to Wassenaar Secretariat*, 14 September 1998. http://www.gilc.org/ Ezekrõl a kockázatokról lásd bõvebben Harold Abelson és mtsai: „The Risks of Key Recovery, Key Escrow, &

tése mellett az Electronic Frontier Foundation a törvénytervezet elõre megjósolható gazdasági következményeire is rámutatott: „A potenciális külföldi vásárlók nem fognak olyan termékeket vagy rendszereket vásárolni, amelyekrõl tudják, olyan »hátsó ajtó« van beépítve, amelyet az Egyesült Államok Kormánya könnyûszerrel ki tud nyitni."[22] Az egyik legtöbb vitát gerjesztett és legnépszerûbb kriptográfiai program, a Pretty Good Privacy (PGP) írója, Philip Zimmermann írásaiban és interjúiban pedig többször utalt arra, hogy mindenekelõtt az *Omnibus Anticrime Bill* (1991) és a *Communications Assistance for Law Enforcement Act* (1994) alapján kibontakozó tökéletesen ellenõrzött társadalom víziója késztette altruista vállalkozásának beindítására. Az utóbbi törvénytervezet ugyanis olyan infrastruktúra kiépítésére kötelezte volna a telekommunikációs szolgáltatókat, amely 1,4 millió telefonvonalon zajló beszélgetés, faxüzenet, e-mail és adatátvitel egyidejû megfigyelését, szûrését tette volna lehetõvé.[23] Ahogy Philip Zimmermann egy rádióinterjúban megfogalmazta: „Nem azért írtam a PGP-t, hogy nagy pénzt keressek vele, hanem hogy a demokráciát tegyem egészségesebbé."[24] A megújuló korlátozási kísérletek következményei leginkább tehát abban mérhetõek, hogy üzleti és altruista vállalkozások százai jöttek létre világszerte, amelyek szabadon megvásárolható vagy ingyen letölthetõ kriptográfiai szoftverek sokaságát kínálják az érdeklõdõknek. A kriptográfiai szoftverek terjedését az is elõmozdította, hogy az erõs kriptográfia amerikai exporttilalma miatt a Microsoft külföldön eladott levelezõprogramjait gyenge, könnyen feltörhetõ védelemmel felszerelve forgalmazhatták. A francia kormány csak többéves hezitálás után, 1999-ben szánta rá magát arra, hogy enyhítsen a kriptográfiai szoftverek használatára és kereskedelmére vonatkozó korábbi szigorú elõírásain. Az 1999. március 17-i *Décret no 99–199* és *Décret no 99–200* megengedi a 128 bit kulcshosszúságú kriptográfiai szoftverek hatósági engedély nélküli és magáncélú használatát.[25] Azonban, úgy tûnik, alaposan elkéstek vele. A nemzetközi és nemzeti korlátozások ellenére ugyanis ma már mintegy másfél ezer kriptográfiai szoftvert kínálnak a világhálón Észtországtól Ausztráliáig; jó részük nem az egyes államok törvényeire és kormányrendeleteire, hanem a világháló használóinak igényeire és szükségleteire való tekintettel kínál-

---

Trusted Third Party Encryption: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists", *Digital Issues,* No. 3. June, 1998.

22 Analysis of the FBI Proposal Regarding Digital Telephony, 1994. http://ftp.eff.org/pub/EFF/Policy/Wiretap/

23 Ahogy a *Security and Freedom through Encryption (SAFE) Act*hez beterjesztett Oxley–Manton-kiegészítés ellen tiltakozó amerikai jogászprofesszorok levelükben rámutattak az állam jogosítványainak korlátaira: „Elfogadjuk azt, hogy a jogalkalmazó szervek lehallgathatják egy személy kommunikációját és lefoglalhatják adatait, amennyiben végrehajtási paranccsal rendelkeznek, s amelynek jogcímét elõzetesen igazolták. De ez a felhatalmazás csak a jogcím megítélése után létezik." *Law Professors' Letter to the House Commerce Committee Opposing Mandatory Key Escrow*, September 23, 1997 http://www.law.miami.edu/~froomkin/lawprof/letter.htm.

24 Russell D. Hoffman's Interview with Philip Zimmermann in the radio show *High Tech Today*, February 2nd, 1996.; Philip Zimmermann, *A Note to PGP Users,* 19 Feb 2001; Steven Levy „Crypto Rebels", *Wired,* 1993. 4.

25 *Décret no 99–199* du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation;

ja erõs kriptográfiai szoftvereit egészen az 512 bit kulcshosszúságúakig. Az említett francia dekrétumokat elõkészítõ kormányzati dokumentum szerzõi egyébként úgy érvelnek, hogy a 128 bit kulcshosszúság „igen magas és tartós védelmet biztosít" a kommunikáció és az elektronikus kereskedelem számára. Ebben valószínûleg igazuk van. Csakhogy az államok és a világháló használóinak-létrehozóinak vitája nem az adatvédelem szükséges és elégséges mértéke körül zajlik, hanem akörül, hogy az állam kötelezõen elõírhatja-e számukra ennek mértékét azzal a nyilvánvaló szándékkal, hogy személyek, szervezetek vagy vállalkozások kommunikációját és adatbázisait akár bírósági felhatalmazás nélkül is folyamatosan ellenõrizhesse. A világháló használóinak-létrehozóinak nagy többsége nem tartja magát ezekhez az elõírásokhoz, más szóval, az alkotmányos jogokkal ellentétesnek tartja azt, hogy az állam a biztonság mértékének meghatározásával próbálja meg kiterjeszteni ellenõrzõ jogosítványait személyes vagy üzleti kommunikációjára és adataira. Talán a határozott elutasítás hatására, s nemkülönben az elektronikus gazdaság és kormányzás biztonságának igénye miatt az európai államok többsége kriptográfiaügyben inkább várakozó álláspontot foglal el, míg mások, különösen Nagy-Britannia – a polgári jog és a büntetõjog alapjait is feszegetõ – kényszerítõ jogi lépésekkel kísérli meg az állam polgáraival szembeni szuverenitását korlátlanul érvényesíteni.[26] Az *Australian Security Intelligence Organization Legislation Amendment Bill* (1999), úgy tûnik, az állami ellenõrzés megvalósításának egy további lehetõségét vázolja fel, amely eleddig a kiberkriminalitás körébe tartozott a világhálón. A törvénytervezet ugyanis a számítógépes adatok és adatforgalom titkos megfigyelése és másolása mellett az adatok változtatására, törlésére és hozzáadására is felhatalmazná a hatóságokat. Igaz, a törvénytervezet szövege homályban hagyja azt a kérdést, hogy milyen adatok változtatására, törlésére és hozzáadására szereznének jogot a hatóságok. Az *Explanatory Memorandum* alapján viszont egyértelmûen arra lehet következtetni, hogy a törvényhozók legalizált crackingra gondoltak, mert az indoklás szerint „az adatok megváltoztatására adott felhatalmazás (powers) segíteni fog a biztonsági rendszerek és a kriptográfiai technikák leküzdésében". Ezt az emelkedett megfogalmazást talán a következõképpen lehet megfejteni: az ausztrál törvényhozás az adatvédelem mértékének állami szabályozása helyett a számítógépes adatokat és szoftvereket manipuláló állami cracking módszerével, vagyis a személyek, szervezetek és vállalkozások számítógépein telepített biztonsági rendszerek kiiktatásával vagy a beállítások manipulálásával kíván

---

Concertation sur le cadre legislatif pour la societe de l'information, Ed. par Ministère de l'Économie, des Finances et de l'Industrie 10/99 Partie III.; Yves Le Roux, *French encryption regulation*, 1998.

26 The OECD's Recommendation of the Council Concerning Guidelines for Cryptography Policy, 27 March 1997.

A kriptográfiai szoftverek szabad kereskedelmét az Európai Unió tagországai közül elsõsorban Nagy-Britannia és Franciaország ellenzi. Az alább idézett cikkek szerzõje szerint az Egyesült Államok tiltakozásának hatására álltak el a kriptográfiai szoftverek szabad exportjától. Lásd ehhez Jelle van Buuren „European Union sets free export of encryption products", *Telepolis*, 22.05.2000 http://www.telepolis.de/english/inhalt/te/8179/1.html; Jelle van Buuren, „European Union postponed decision on removing barriers to Export of Crypto," *Telepolis*, 25.05.2000 http://www.telepolis.de/english/inhalt/te/8192/1.html.

az állami ellenõrzésnek érvényt szerezni.[27]

Tévedés lenne azonban a kriptográfia kérdésében mutatkozó határozatlanság, az államok konszenzushiánya és szembenálló érdekei alapján arra következtetni, hogy az Európai Tanács s az európai államok egy része lemondott volna a világhálón folyó kommunikáció és a kommunikáló személyek totális ellenõrzésének a megvalósításáról. Az Európai Tanács 2001. március 30-án kelt dokumentuma, az *ENFOPOL 29* ennek a személyekre és tartalmakra kiterjedõ totális ellenõrzésnek a technikai kereteit vázolja fel (ha egyáltalán beszélhetünk keretekrõl minden kommunikációs tartalomra és minden kommunikáló személyre kiterjedõ, jelen idejû és élettörténeti ellenõrzés esetében).[28] Ez a dokumentum – az eredeti politikai szándék fenntartása mellett – tulajdonképpen technikai szempontból fogalmazza újra és pontosítja a fent idézett *Resolution on the Lawful Interception of Telecommunications* (1995) iránymutatásait. A technikai átdolgozásra és pontosításra mindenekelõtt azért került sor, mert a döntéshozók úgy vélték, hogy az információs eszközök, technikák és technológiák fejlõdése néhány év alatt túllépett az 1992-es *International User Requirements* címû FBI-dokumentumban megfogalmazott és 1995-ben az Európai Unió által is kodifikált szándékokon.[29] Mintha a döntéshozók csak most értették volna meg a kommunikáció forradalmának jelentését, mintha csak most tudatosodtak volna számukra a kommunikációs tartalmak digitalizációjának a kommunikációs univerzum egészét érintõ technikai és társadalmi következményei. A jelek digitalizációja tette ugyanis lehetõvé a jeltovábbítás korábban elválasztott csatornáinak egységesítését, ez nyitotta meg az utat a kommunikáció eszközeinek, technikáinak és technológiáinak a konvergenciája elõtt, s nem utolsósorban ennek következtében vált megvalósíthatóvá az input és az output között áramló digitális jelek (kommunikációs tartalmak és átviteli adatok) teljes körû, számítógépek által végzett kibernetikus kontrollja. Persze a kommunikációs tartalmak és átviteli adatok nemcsak a számítógépek, hanem a számítógépeket és az átvitel különbözõ csatornáit birtokló politikai és gazdasági szervezetek számára is ellenõrizhetõvé, rögzíthetõvé, manipulálhatóvá, analizálhatóvá és szûrhetõvé váltak. Ezért az *ENFOPOL 29* a szolgáltatás típusától, a jeltovábbítás csatornáitól, az alkalmazott eszközöktõl és technikáktól, a kommunikáció módja-

---

27 Australian Security Intelligence Organization Legislation Amendment Bill (1999) in Bills Digest No. 172, 1998–99.

28 Council of the European Union „Law enforcement – Operational needs with respect to public telecommunication networks and services", Brussels, 30 March 2001 7616/01 (*ENFOPOL 29*, Brussels, 30 March 2001). Vö. Council of the European Union „Relations between the first and third pillars on advanced technologies", Brussels, 31 October 2000.; *ENFOPOL 71 REV 1*, Brussels, 27 November 2000.

29 *ENFOPOL 98,* Brussels, 3 September 1998; *ENFOPOL 98 REV 1*, Brussels, 10 November 1998; *ENFOPOL 98 REV 2*, Brussels, 3 December 1998. A *Resolution on the Lawful Interception of Telecommunications* (1995) keletkezéstörténetéhez lásd: http://www.statewatch.org/news/2001/may/ILETS99-report.doc; Duncan Campbell „Special Investigation: ILETS and the ENFOPOL 98 Affair", *Telepolis*, 29.04.1999.; Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, 1998.184. Az Európai Unió adatvédelmi biztosai egyébként számos dokumentumban utalnak a *Resolution on the Lawful Interception of Telecommunications* (1995) legalitásának

itól, a küldõ és a címzett személyek és szervezetek helyétõl és jogalanyiságától függetlenül már egységesen kezeli a digitalizált kommunikációs tartalmakat és átviteli adatokat. Az Európai Tanácsnak az *ENFOPOL 29*-ben kifejtett elképzelései szerint tehát a szolgáltatóknak (ISP, CSP) a digitalizált kommunikációs tartalmak és átviteli adatok egészét, vagyis minden egyes vezetékes, mûholdas, internetes és mobil telefonhívást, faxüzenetet, e-mailt, weboldaltartalmat és azok változásait, minden adatbázist, adatforgalmat, s az adatcsomagokhoz, az eszközökhöz, valamint a kommunikáló személyekhez tartozó valamennyi azonosítót elõzetes bírósági felhatalmazás nélkül kellene hozzáférhetõvé tenni, automatikusan rögzíteni, és legalább tizenkét hónapig archiválni a hatóságok számára.[30] Az idézett dokumentumok ugyanakkor igyekeznek határozottan elválasztani egymástól a kommunikációs tartalmakat a forgalmi adatoktól, s hangsúlyozzák, hogy az adatok folyamatos, kötelezõ és általános rögzítése – a hagyományos telefonszolgáltatók esetében szokásos számlázáshoz hasonlóan – kizárólag a forgalmi adatokra fog majd kiterjedni. A kibertérben azonban alapvetõen csomagkapcsolt kommunikáció zajlik, ezért megtévesztõ az analóg telefonhálózat mûködését példaként felidézni. A csomagkapcsolt kommunikáció esetében a csomag, a fejléccel ellátott rövid bitsorozat egyszerre és elválaszthatatlanul foglalja magába a tartalmat és a forgalmi adatokat. Ez utóbbiak a csomag azonosítói, vagyis az üzenet küldõjének és címzettjének címét, az útvonalat, az üzenet keletkezésének idejét, a küldés idõtartamát, az üzenet formátumát és az egyes csomagok összeállításának speciális algoritmusát tartalmazzák. Mindezekre egyszerre van szükségünk ahhoz, hogy ezek a csomagok jelen idejû vagy archivált akusztikus/auditív vagy vizuális, képi vagy textuális üzenetekké álljanak össze számítógépünkön. Ahogy az Egyesült Államokban a *Communications Assistance for Law Enforcement Act* (1994) vitája során is megválaszolat-

---

általános problémáira. Lásd ehhez például: *Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications,* Brussels, 3 May 1999.

30 *ENFOPOL 29*, Brussels, 30 March 2001.

A kommunikációs tartalmak és átviteli adatok megõrzésének idejére vonatkozóan nincs egyetértés a tagállamok között. Míg Hollandiában az Európa Tanács javaslatával összhangban 3 hónapig, addig a spanyol törvénytervezet, a *Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (2001) szerint a szolgáltatóknak „legfeljebb hat hónapig" (art. 11d.) kell megõrizniük ügyfeleik kommunikációs és átviteli adatait. Viszont a belga *Loi du 28 novembre 2000 relative à la criminalité informatique* Ch IV. art. 12., s ugyanígy a francia törvénytervezet, a *Loi sur la société de l'information* (2001) is legalább 12 hónapos kötelezettséget ró a szolgáltatókra.

Egy angol javaslat szerint az adatokat 12 hónapig a szolgáltatóknak kellene megõrizniük, majd ezután azokat úgynevezett adatraktárakban hat évig archiválni. Az adatraktárak felállításának és mûködtetésének költségeit a szolgáltatóknak (persze, végsõ soron ügyfeleiknek) kellene viselniük, illetve – a tervezet írója szerint – az adatraktárak fenntartását üzleti, afféle adatkereskedelmi vállalkozások kezébe lehetne adni. Roger Gaspar, *Looking to the Future Clarity on Communications Data Retention Law Submission to the Home Office for Legislation on Data Retention*, 21st August 2000; Ian Black, „Alarm at European data surveillance plan", *The Guardian*, 18 May 2001; Kamal Ahmed, „Secret plan to spy on all British phone calls", *The Observer*, Sunday December 3, 2000.

31 A technikai részletekhez lásd például Robin Burk and David B. Horvath, CCP, et al. *UNIX Unleashed, System Administrator's Edition*, Macmillan Computer Publishing, Online edition, 1997. Chs 7. és 20.; és *CALEA Flexible Deployment Assistance: Packet-Mode Communications Guide,* 2nd

lanul maradt az a kérdés, hogy miként fogják majd elválasztani egymástól a kommunikációs tartalmakat a forgalmi adatoktól, ugyanúgy az idézett *ENFOPOL*-dokumentumokban sem találunk ezzel kapcsolatban semmiféle jogi vagy technikai útmutatást.[31] Ez a látszólag száraz és unalmas technikai szõrszálhasogatás azonban a kommunikációs és információs szabadság korlátozására tett kísérlet lényegét érinti. Ugyanis míg a kommunikációs tartalmak titkos megfigyelésének és rögzítésének engedélyezését a demokratikus társadalmakban egyedi esetek gondos vizsgálatán alapuló különleges bírói felhatalmazáshoz kötik és ritkán alkalmazzák, addig most a világháló technikai jellegzetességébõl következõen a megfigyelés és a rögzítés mindenkire kiterjedõ, egyszerû rutinfeladattá válhat. Talán nem szükséges különösebben hangsúlyozni, hogy e terv megvalósításának a demokratikus politikai berendezkedés alapjait érintõ következményei lennének. Az Európai Tanács idézett dokumentumainak szerzõi a teljes körû adatgyûjtés politikai filozófiai, nemzetközi jogi, alkotmányjogi vagy emberi jogi vonatkozásaival egyáltalán nem foglalkoznak. Mindenképpen különös, hogy nem tartották feladatuknak egy ilyen általános politikai-jogi kényszer alkalmazására tett javaslat elméleti megalapozását és szükségességének gyakorlati igazolását. Mindenekelõtt meg kellett volna magyarázni, hogy a kommunikációs tartalmak és átviteli adatok totális megfigyelésének, rögzítésének és archiválásának jogi kényszerét miért terjesztik ki a társadalom egészére, a megfigyelés, rögzítés és archiválás miért vesz célba olyan embereket, akiknek többsége nem vét a törvény ellen, és akikkel szemben ilyen gyanú fel sem merült. A kommunikáció totális ellenõrzésére és az információs szabadság korlátozására tett javaslat általánosan korlátozza a világhálón zajló gigantikus párbeszédbe bekapcsolódó emberek politikai jogait, amelyeken egyébként a demokratikus társadalmakban az állam mûködésének és jogosítványainak legitimitása is alapszik.

Az idézett dokumentumok ugyanakkor csak érintõlegesen foglalkoznak azzal a kérdéssel, hogy melyek azok a társadalomra leselkedõ közvetlen és súlyos veszélyek, amelyeket állami kényszerek alkalmazásával, a kommunikáció és információ szabadságának korlátozásával, vagy bizonyos beszédmódok kriminalizálásával lehet csak elhárítani. Az *ENFOPOL 71 REV 1*-ben a megfigyelés szükségessége mellett felhozott esetek többsége például egyáltalán nem tartozik az információs technológiával és számítógéppel kapcsolatos bûnözés körébe.[32] Azonban a valóságos problémák alapos és részletes számbavételének hiánya, a kommunikációs univerzum kiszélesedésébõl eredõ veszélyek diabolizálása és az elnagyolt tárgyalásmód korántsem véletlen. Az Európai Bizottság *Creating a Safer Information Society* (2000) címû közleményének állítása szerint: információs technológiával és számítógéppel kapcsolatos bûnözésre vonatkozó, megbízható és teljes körû statisztikák nem állnak rendelkezésünkre, a legtöbb országban számítógép- és a kommunikációs rendszerek használatára vonatkozó bûnügyi statisztikákat a hatóságok nem is készítenek.[33]

---

ed. August 2001.; Oscar S. Cisneros, „These Wires Were Made for Tapping", *Wired News*, 3:00 a. m. Aug. 14, 2000 PDT.

32 *ENFOPOL 71 REV 1*, Brussels, 27 November 2000.

33 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Communication from the Commission to the Council, the

Az *ENFOPOL 38* szerint a kiberkriminalitás felmérésére vonatkozó rendszeres és átfogó statisztika készítését elõször 2000-ben kezdeményezték.[34] Az ott közölt rövid statisztikai összegzés összeállítói maguk is utalnak rá, hogy a számadatok nem alkalmasak – többek között a durva kategóriahibák, a komprehenzivitás, a világos és egyértelmû szempontok hiánya miatt – általános következtetések levonására. Röviden, az *ENFOPOL*-dokumentumokban megfogalmazott következtetések sokkal inkább vélekedéseken, egyedi esetek általánosításán és megalapozatlan sajtóhíreszteléseken, mintsem tényeken, átfogó vizsgálatokon alapulnak.[35]

Az alapvetõ elméleti és gyakorlati kérdések felvetése helyett az *ENFOPOL 29* inkább a személyes adatok és a magánélet védelmére vonatkozó közösségi jogok szûkítésére és ajánlások visszavonására tesz javaslatokat. Az adatvédelem kérdéseivel foglalkozó egyezmények és határozatok – így például, a *Convention ETS N° 108*, a *Directive 95/46/EC*, a *Directive 97/66/EC* és a *Directive 2000/31/EC* – ugyanis határozottan tiltják a kommunikációs tartalmak és a személyek azonosítására szolgáló adatok totális megfigyelését, rögzítését és archiválását, s ebben a vonatkozásban szigorú elõírásokat fogalmaznak meg az információs és kommunikációs szolgáltatók, az üzleti vállalkozások és szervezetek, s ugyanúgy a hatóságok számára is. Ahogy az

---

European Parliament, etc. Brussels, 2000. 11.

34 *ENFOPOL 38*, Brussels, 24 April 2001.

35 A megalapozatlan sajtóhíreszteléshez lásd például a londoni *Observer* 1996. augusztus 25-i címlapsztoriját. Az újság, bizonyos amerikai FBI-szakértõkre és a finn rendõrségre hivatkozva, azzal vádolta meg Johan „Julf" Helsingiust, hogy az internetes vállalkozása által mûködtetett anonim remail szerver, az anon.penet.fi „az interneten lévõ gyermekpornográfia 90 százalékának középpontja". Az újság által közölt állítások és rendõrségi hivatkozások, mint azt a rendõrségi vizsgálatok és cáfolatok is megerõsítették, csupán a cikk írójának konfabulációja volt. Éppen a finn rendõrség kérésére az anonim remail szerver – egy 386-os, 200 MB winchesterrel rendelkezõ öreg masina – 16 kilobytenál hosszabb levelet nem fogadott, így az képek továbbítására nem is volt alkalmas.

Ugyancsak szenzációs leleplezést ígért az amerikai *Time* magazin címlapsztorija, az „On a Screen Near You: Cyberporn" (July 3, 1995 Volume 146, No. 1). A szerzõ, Philip Elmer-DeWitt cikkében többször utal arra, hogy állításai és adatai a Carnegie-Mellon University kutatóinak jelentésén alapulnak. Elmer-DeWitt szerint a kutatók, akik 18 hónapig tartó kutatómunkával „917 410 szexuálisan egyértelmû képet, leírást, történetet és filmklipet tanulmányoztak", többek között arra a megállapításra jutottak, hogy a Usenet hírcsoportok által tárolt képek 83,5%-a pornográf. Mint késõbb kiderült, ilyen kutatócsoport nem mûködött az egyetemen, s értelemszerûen ilyen kutatást senki sem végzett. A cikk egy elsõéves villamosmérnök hallgató, Martin Rimm adatait tekintve manipulált, számításaiban hibás és következtetéseiben megalapozatlan szemináriumi dolgozatán, a „Marketing Pornography on the Information Superhighway"-en alapult. Elmer-DeWitt késõbb azzal mentegetõzött, hogy titoktartási szerzõdést írattak vele alá, így nem állt módjában szakértõkkel ellenõriztetni Rimm állításait, továbbá, hogy a hetilapok õrült hírversenyében neki hétrõl hétre kell szenzációs híreket szállítania olvasóinak. Kétségtelen, hogy cikke ez utóbbi elvárásnak meg is felelt. A közgondolkodásban azóta is makacsul tartja magát a „Rimm Factor", nevezetesen, hogy a világhálón található képek 80%-a pornográf. Lásd ehhez Donna L. Hoffman–Tom Novak „A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: »Marketing Pornography on the Information Superhighway«", http://www2000.ogsm.vanderbilt.edu/novak/rimm.review.html; Brock N. Meeks, „Point-Five Percent Solution: Time magazine's credibility is hemorrhaging", *CyberWire Dispatch*, 7 July 1995. http://cyberwerks.com/cyberwire/cwd/cwd.95.07.04.html; Brock N. Meeks, „Muckracker: Over the Top and Into the Rimm", HotWired, *24 July 1995.*

Európai Unió adatvédelmi biztosai a *Convention on Cyber-crime* (2001) egy korábbi változata kapcsán ajánlásukban megfogalmazták: „A széles körû felderítést vagy általános megfigyelést be kell tiltani. Ebbõl következik, hogy a hatóságok számára csak esetrõl esetre engedélyezhetõ az átviteli adatokhoz való hozzáférés, sohasem proaktív módon és sohasem általános szabályként."[36] Az *ENFOPOL 71* tanúsága szerint a Working Party on Police Cooperation belga, német, francia, holland, svéd és angol delegátusai „nyugtalanságukat fejezték ki" amiatt, hogy az új adatvédelmi irányelvek tervezete is tartalmazza a *Directive 97/66/EC* 6. cikkét, vagyis azt, hogy „a használókra és az elõfizetõkre vonatkozó forgalmi adatokat, amelyeket a nyilvános kommunikációs hálózat vagy szolgáltatás fenntartója dolgozott fel és tárolt az üzenet továbbítása céljából, a továbbítás befejeztével törölni vagy névteleníteni kell".[37] A hivatalos dokumentumok alapján arra lehet következtetni, hogy a kommunikációs adatok megfigyelésének, rögzítésének és archiválásának kérdésében az Európai Unió államainak kormányai és intézményei meglehetõsen megosztottak. A tanulmány írója elképzelni sem tudja, hogy miféle áthidaló megoldást lehetne találni az információ és a kommunikáció szabadságát és személyességét védelmezõ, és a kommunikációs univerzum totális ellenõrzésének bevezetését szorgalmazó államok álláspontja között?[38] Legalábbis Tocqueville a 19. században még úgy vélte, hogy nincs köztes állapot a beszéd szabadsága és a szolgaság között.

Mint már hangsúlyoztam, a világháló kommunikációs tere a nem lokalitás elvén mûködik. A kommunikációs univerzum olyan nyelvi, társadalmi és politikai tér, amelyre az egyes államok vagy államszövetségek joghatósága és szuverenitása egykönnyen nem terjeszthetõ ki. Ez a nyelvi, társadalmi és politikai tér, amelyet az emberek, valamint az emberek és a gépek közötti kommunikáció pillanatról pillanatra hoz létre, nem parcellázható fel a hagyományos területi joghatóságok és szuverenitások szerint. Az államok persze nem akarják tudomásul venni területi joghatóságuk és szuverenitásuk korlátozását, esetleg kiüresedését a kibertérben, s ezért azt különbözõ módokon igyekeznek megakadályozni. A világháló mûködésének egységes nemzetközi jogi szabályozása helyett – amelynek egyébként a nemzeti jurisdikciók, az értékek és az érdekek különbözõsége miatt igen csekély a va-

36 Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, Brussels, 7 September 1999.

37 *ENFOPOL 71 REV*, Brussels, 27 November 2000. Vö. *Directive 97/66/EC* Art. 6.

38 Letter of the Article 29 Data Protection Working Party to the Acting President of the Council of the European Union, (The Rodotà-letter) Brussels, 7 June 2001.; Report from General Secretariat to COREPER, Brussels, 31 May 2001.

39 Például Claudia Nolte német családügyi miniszter 1996. július 16-án az ENSZ-ben kezdeményezte azoknak a nemzetközi alapelveknek a kidolgozását, amelyek segítségével megakadályozható lenne az újnáci nézetek és a pornográfia online terjesztõinek a nemzeti joghatóságokon kívüli tevékenysége. Rose Aguilar, „Germany asks U.N. for Web guidance", *CNET News.com*, July 17, 1996, 1:30 p. m. PT. Lásd ezzel szemben Adam Tanner, „Germany won't block access to foreign Nazi sites", *Silicon Valley News*, 25 July 2000.

40 Ennek az „effects based jurisdiction"-nek az ellentmondásait elemzi Michael Geist, „Everybody Wants to Rule the Web", *Globe and Mail*, 18 January 2001, http://www.globetechnology.com/archive/gam/E-Business/20010118/TWGEIS.html A Yahoo! Inc.-hez lásd Tribunal de Grande Instance de

lószínûsége a közeli jövõben[39] – az egyes államok inkább joghatóságuk és szuverenitásuk nyílt vagy burkolt területi kiterjesztésével próbálkoznak. Azonban, ahogy a kaliforniai Yahoo! International ellen hozott francia bírósági ítélettel szembeni amerikai, vagy az orosz programozó, Dimitrij Szkljarov amerikai letartóztatása elleni nemzetközi tiltakozás mutatja: a világháló társadalma nem tudja elfogadni az egyes államok egyoldalú lépéseit, amelyek végsõ soron a kommunikációs univerzum politikai, földrajzi és jogi szegmentálásához vezetnének.[40] Érdekes lenne az a megoldás – ami egyébként a francia bíróságnak a Yahoo! International ellen hozott következményelvû („effects based") ítéletébõl következik –, ha egy és ugyanazon információs és kommunikációs tartalmakat egyidejûleg kétszázféle nemzeti jurisdikciónak kellene alárendelni. Illetve, ha a technológiára hagyatkozva kétszázféleképpen konfigurált, államilag elõírt szûrõprogram terelgetné a felhasználókat állampolgárságuk szerint jogszerûnek és decensnek ítélt tartalmak felé. Mindenesetre a világháló használóinak lokalizációja és ennek megfelelõen az információs és kommunikációs tartalmak létrehozásának és hozzáférhetõségének állami szabályozása, ellenõrzése és szûrése alapvetõen írná át az internet „end-to-end" architektúráját, amelybõl egyébként a rendszer mûködésének és fejlõdésének dinamikája fakad.

Az *ENFOPOL 29* javaslatai sajátos módon próbálnak túllépni a kibertér és a földi tér közötti jogi és politikai földrajzi konfliktusokon. Az *ENFOPOL 29* ugyanis olyan kommunikációs tartalmak és átviteli adatok megfigyelésére, rögzítésére és archiválására is kiterjed, amelyek küldõje és fogadója nem az Európai Unió valamely államának polgára vagy valamely államában bejegyzett és annak területén mûködõ szervezet. A világháló mûködésének logikájából következõen az üzenetek országok sokaságán – így az Európai Unió országainak területén mûködõ szervereken és forgalomirányító számítógépeken – haladnak át. A kommunikációs és átviteli adatok ugyanis nincsenek tekintettel az országhatárokra, azok a gépek által meghatározott optimális útvonalon haladnak céljuk felé. Az idézett *ENFOPOL 29* mellett kifejezetten ezt ajánlja az angol belügyminiszter figyelmébe Roger Gaspar, a *Looking to the Future: Clarity on Communications Data Retention Law* (2000) szerzõje: „A törvényhozásnak valamennyi kommunikációs szolgáltatót (CSP) arra kell köteleznie, hogy az Egyesült Királyságból származó vagy oda irányuló, vagy az Egyesült Királyság hálózatain áthaladó összes kommunikációs adatot megõrizze, beleértve azt is, amelyet külföldön tárolnak."[41] Röviden, ezek a javaslatok azt szorgalmazzák, hogy az Európai Unió vagy Nagy-Britannia terjessze ki illetékességét az unió vagy az ország határain kívül élõ polgárok és szervezetek kommunikációjára, külföldi adatbázisaira is. A *Convention ETS Nº 108*-ból ugyanakkor az következik, hogy a kommunikációs és átviteli adatok puszta áthaladása nem ad felhatalmazást egyik állam számára sem azok megfigyelésére, rögzítésére és archiválására. Az Európai Unió tisztségviselõi, az Eu-

---

Paris: Ordonnance de référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo! France*, http://www. juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm.

41 Roger Gaspar, *Looking to the Future: Clarity on Communications Data Retention Law*, Submission to the Home Office for Legislation on Data Retention, 21st August 2000.

rópa Parlament képviselõi mindig érzékenyen reagáltak azokra a hírekre és esetekre, amikor felmerült annak a gyanúja, hogy egy másik országban mûködõ üzleti vállalkozás vagy hatóság az EU polgárainak, szervezeteinek és üzleti vállalkozásainak kommunikációs és átviteli adatait figyelte, rögzítette, archiválta, vagy az adatokkal kereskedett. Ezeket az eseteket a személyes adatok védelmére vonatkozó saját belsõ, és a nemzetközi jogrend kontextusában is értékelte, s ezeknek a szigorú szabályoknak az érvényesítését követelte meg a külföldi hatóságoktól, szolgáltatóktól vagy vállalkozásoktól is polgárai érdekében.[42] A *Convention ETS Nº 108* 12. cikkének III. fejezete szerint az államoknak fel kell lépniük polgáraik személyes adatainak védelmében, s az adatok országhatárokon áthaladó szabad áramlását akár meg is tilthatják vagy speciális szabályokhoz köthetik akkor, ha egy másik országban azokat nem részesítik hasonlóan szigorú védelemben.[43] Ezért a nemzeti és nemzetközi jogrend kontextusában vizsgálva az *ENFOPOL 29*-ben megfogalmazott javaslatok az Európai Unió országait sajátos, Russell borbélyparadoxonját idézõ helyzetbe hozzák.[44] A javaslat elfogadása következtében ezek az adatok nem részesülnének védelemben – hiszen az állam a kommunikációs tartalmak és átviteli adatok folyamatos és proaktív megfigyelésére, rögzítésére és archiválására tesz javaslatot függetlenül a kommunikáló személyek és szervezetek helyétõl és jogalanyiságától –, de éppen a védelem hiánya miatt az államnak polgárai biztonsága érdekében egyúttal tiltania vagy korlátoznia kellene a személyes adatok országhatárokon áthaladó forgalmát.

Technológia és a kibertér kommunikatív architektúrája

Azok a törekvések, amelyek a hatékony állami ellenõrzés érdekében a világhálót mûködtetõ és biztonságát szolgáló technikák és technológiák korlátozására vagy monopolizálására irányulnak, nem tûnnek életképes megoldásoknak. A világháló ugyanis nem központi terv eredményeként valósult meg, s ma sincs központi informatikai agytrösztje. A világhálót különbözõ, egymással többé-kevésbé kompatibi-

42 Directive 95/46/EC §§ 56–61.; ETS No 108. art. 12.; Draft Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception **[42. folyt.]** System), Temporary Committee on the ECHELON Interception System the European Parliament, Rapporteur: Gerhard Schmid, 18 May 2001.; Privacy on the Internet – An integrated EU Approach to On-line Data Protection, Adopted on 21st November 2000.; Proposal for a Directive of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, Brussels, 12 July 2000.; Network and Information Security: Proposal for a European Policy Approach**,** Communication from the Commission to the Council, etc. Brussels, 2001.; Chair's Conclusions of G–7 Ministerial Conference on the Information Society, Brussels, 26 February 1995.; Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society, 1998. 116. 25–27., 62–68.

43 Convention ETS Nº 108 Ch. III. Article 12; The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980. C(80)58(Final); Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS Nº 108) Strasbourg, 8 June 2000.

lis és egymással keményen versengõ technikai megoldások és technológiák sokasága hálózza be és mûködteti. A technikai fejlõdés irányát még rövid távon is nehéz elõre jelezni, de az elég nyilvánvalónak látszik, hogy a szabályozást és korlátozást szolgáló politikai-jogi eszközök a folyamatos technikai és technológiai változásokkal nemigen tudnak lépést tartani. A technikai jellegû korlátozásokkal és a technikára bízott ellenõrzéssel szemben mindig lehet jobb technikával, elegáns és innovatív informatikai megoldásokkal védekezni. Ne feledjük, a világháló társadalmának tagjai képzettek és járatosak a digitális kultúra világában, hiszen õk hozzák létre azt, õk rendelkeznek az információk, a feladatok és a megoldások disztribúciójából eredõ elõnyökkel. Látszólag jelentéktelen, viszonylag egyszerû, de fénysebességgel terjedõ ötletek és megoldások – például a PGP, a Napster, a Gnutella, a Free Network Project, a Publius, a P2P, a Grid és hasonló elképzelések – idõrõl idõre átírják a világháló mûködésének technikai és társadalmi feltételeit, s új lehetõségeket nyitnak meg a használók-létrehozók elõtt.[45] Az Európa Tanács idézett tervezete a jelenleg még domináns kliens-szerver viszonyra építve az internetszolgáltatókon keresztül akarja megvalósítani a totális állami ellenõrzést. Logikus lépésnek tûnik ez, hiszen a szolgáltatók számítógépei, a szerverek végzik a címek, a tranzakciók és az adatforgalom technikai adminisztrációját. S miért ne végeztethetnék el velük a személyek és az adatok folyamatos gyûjtésének, ellenõrzésének és cenzúrázásának fáradságos munkáját? De ami logikusnak és technikailag kivitelezhetõnek tûnik most, nem biztos, hogy az is marad. Mert a kívülrõl diktált és sokakban a totálisan ellenõrzött társadalom rémképét idézõ beavatkozások olyan technikai és technológiai változásokat generálnak, amelyek a közeli jövõben elvezethetnek a kliens-szerver viszony lebontásához. Ahogy Ian Clarke, a Free Network Project alapítója megfogalmazta: „A Freenet Network az Internethez kapcsolódó számítógépek sokaságából áll, amelyek egy kis »Freenet Server« vagy »Freenet Daemon« programot futtatnak. E program lehetõvé teszi azt, hogy a számítógép a hálózat csomópontjává, az egész hálózat kicsi, de egyenlõ részévé váljon. A Freenet valójában a tökéletes anarchia".[46] A digitális kultúra avantgárdja a hatalmat gyakorló arkhónok nélküli állapotként képzeli el a világháló jövõjét. S az „egyenlõ az egyenlõhöz" (Peer-to-Peer, P2P), vagy az önkéntesek társulásán alapuló Grid hálózati architektúra sokkal inkább megfelel egy demokratikus társadalom alapelveinek. Ezért könnyen elképzelhetõ, hogy mire az egyezményt a tagállamok aláírják, s az aláíró tagállamokban életbe lép, már jogtörténeti dokumentummá válik.

A világháló használóinak-létrehozóinak elképzelései és a politika szándékai közötti konfliktusok leginkább tehát arra vezethetõk vissza, hogy az egyes országok törvényhozásai függetleníteni akarják magukat a világháló mûködésének emberi és technikai alapelveitõl, de – mint láttuk – különféle veszélyekre hivatkozva a demokratikus társadalmak évszázados jogelveitõl is. A korábbiakban igyekez-

44 Russell paradoxonja szerint a falusi borbély az a személy, aki azokat a falubelieket borotválja, akik nem maguk borotválkoznak. De ha a borbély azok közé tartozik, akik maguk borotválkoznak, akkor nem a borbély borotválja? Vagy ha a borbély borotválja, akkor nem maga borotválkozik?

45 http://cs1.cs.nyu.edu/waldman/publius/ http://gnutella.wego.com/ http://freenet.sourceforge.net/

tem rámutatni a participáción és a konszenzuson nyugvó alapelvek fontosságára. Ugyanakkor a világháló mûködésének és dinamikus növekedésének vannak más szükségszerû, a tudás egyenlõ disztribúciójára, a rendszer performativitására és funkcionalitására vonatkozó feltételei is. E globális és dinamikus rendszer szabályait a használók-létrehozók kommunikatív cselekvései írják; s mivel ennek a gigantikus diszkussziónak „mindenki minden pillanatban részese, ezért mindenki szüntelenül hat rá" (Saussure 1972: 107). A használó-létrehozó személyek interakciói a tudás szabad létrehozására, áramlására és értelmezésére, vagyis a globális és dinamikus rendszer performativitására és funkcionalitására való tekintettel keresik a mûködés optimális feltételeit. Ezért a kommunikáció szabad áramlásának, vagyis a rendszer performativitásának és funkcionalitásának igénye szinte elõre kódolja a külsõ, statikus és megszorító szabályozási törekvések kudarcát; mindazokét, amelyek a globális és dinamikus rendszer mûködése elé mesterséges politikai, jogi és gazdasági akadályokat igyekeznek állítani. Bármennyire nehéz is kulturálisan feldolgoznunk, tudomásul kell vennünk azt, hogy a kiberteret paradoxonok egész sora hozza létre és mûködteti. A kibertér a használó-létrehozó számára valóságos kommunikatív tér, mégis virtuális, mert földrajzilag nem lokalizálható. Olyan globális társadalmi tér, amely nem az egyes államok határain belül fekszik, így az egyes kormányzatok a kibertér felett nem tudják hatékonyan és eredményesen gyakorolni joghatóságukat és területi szuverenitásukat. Ebben a térben a használók-létrehozók interakciói hozzák létre a kommunikáció szabályait, de a szabályok nem rögzíthetõk, ugyanakkor önkényesen nem is változtathatók, mert „a változás elve a folytonosság elvén alapszik" (Saussure 1972: 109). A globális rendszer egésze középpont nélküli, mégis a használó-létrehozó saját kompetenciája szerint generálja önmaga mint középpont körül a tudás változatos alakzatait. Más szóval, az egészbõl olyan részhalmazokat hoz létre, amelyek egyediek, mert saját kommunikatív kompetenciáját tükrözik, saját helyesség- és hasznosságigényének felelnek meg, de mégsem önkényesek, mert a kommunikáció performativitása, a jelentések interszubjektív megragadhatósága érdekében a használó-létrehozónak mindig tekintettel kell lennie a közös kommunikatív tér nyelvi-kulturális szabályaira.

*

A személy identitásának és a digitalizált tartalmaknak a transzparenciája, a kommunikáció kibernetikus kontrollja és e kontroll hatalmi-gazdasági kontrollja sokakban idézi fel Bentham *Panopticon*jának vagy Orwell *Big Brother*jének vízióját. A törvények és a törvénytervezetek azon törekvései, amelyek a közszabadság jogelveinek figyelmen kívül hagyása és a drákói büntetési tételek bevezetése mellett a kommunikációs tartalmak szûrésére, a teljes körû és folyamatos adatgyûjtésre, bizonyos algoritmusok különleges védelmére és mások tiltására irányulnak, sokak számára igazolják azt, hogy Bentham, Kafka, Orwell és Atwood intézményei és figurái nem pusztán klasszikus irodalmi reminiszcenciák vagy hétköznapi paranoiák szülöttei voltak. Igaz, Bentham és *Panopticon*ja nem sorolható a disztópikus irodalom nagy vonulatába. Bentham ugyanis, üzleti sikereinek elõmozdítása mellett,

a társadalom megreformálását, a társadalmi deviancia leküzdését és a morál védelmét remélte különös terve megvalósításától. Hasonlóképpen érvelt egykor, mint az információ és a kommunikáció tökéletes állami kontrolljának és a társadalmi transzparenciának a mai képviselõi. Ahogy David Lyon megfogalmazta: „Bentham Panopticonja az isteni mindentudás világi paródiáját képviselte, a megfigyelõ, mint az Isten, láthatatlan maradt" (Lyon 1994: 57–80). Mindenesetre, az istent játszó Bentham üzleti terve, Kafka, Orwell és Atwood disztópikus irodalmi víziói könnyen valósággá válhatnak egy olyan társadalomban, ahol az új kommunikációs technológiák teljesen behálózzák a személyek közötti kommunikáció virtuális tereit, és amelynek polgárai nem lépnek fel a kommunikáció és az információ szabadságának védelmében.[47]

Hivatkozott irodalom

Akdeniz, Yaman és Caspar Bowden (1999): Cryptography and Democracy: Dilemmas of Freedom. In *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet*. London.

Anderson, John Ward (2001): Turkey in a Tangle Over Control of Web. In *Washington Post,* jún. 21., A19.

Barbrook, Richard és Andy Cameron (1997): A kaliforniai ideológia. In *Buldózer: Médiaelméleti antológia*. Budapest.

Barlow, John Perry (1990): Crime and Puzzlement: Desperados of the DataSphere. In *Whole Earth Review*. Fall.

Bingham, Eugene (2001): Police snooping needs tight rein says report. In *New Zeeland Herald Online,* jan. 3.

Bogád Zoltán (2001): Szexmentes a magyar honatyák hálózata. In *Index*, március 23., péntek, 17: 06.

Bowden, Caspar (1999): Decrypt with Care. In *Financial Times*, december 21.

Coffman, K. G. és A. M. Odlyzko (2001): Internet growth: Is there a „Moore's Law" for data traffic? In *Handbook of Massive Data Sets*. J. Abello és mtársai (szerk.). Hague: Kluwer.

Dearne, Karen (2001): Censor Bill gets R rating. In *Australian IT,* február 27.

Gauthronet, Serge és Etienne Drouard (2001): *Communications Commerciales Non-Sollicitées et Protection des Données.* Paris.

Herzlich, Guy és Françoise Vaysse (1993): La crise de la consommation est une crise de l'immatériel: Un entretien avec Robert Rochefort. In *Le Monde,* július 6., 2.

Isler, Thomas és Oliver Zihlmann ((2001): WEF-Gegner stahlen Geheimdaten der Mächtigen Hacker kopierten illegal Kreditkartennummern, Pass-, Handy- und Privatnummern von 1400 Wirtschaftsführern. In *Sonntags Zeitung,* febr. 4. http://www.sonntagszeitung.ch

---

http://gnutella.wego.com/ http://www.napster.com/pressroom/pr/napster/rebuttal.html

46 Richard Koman „Free Radical: Ian Clarke has Big Plans for the Internet", 11/14/2000 http://www.oreillynet.com/p2p/

47 Duncan Campbell, Interception Capabilities 2000: Report to the Director General for Research of the European Parliament, Edinburgh, April, 1999; Big Brother in the Wires: Wiretapping in the Digital Age, An ACLU Special Report, March 1998; Communication: For and Against Democracy, Ed. Mark Raboy and Peter Bruck, Montreal-New York, 1989; Kevin Robins and Frank Webster, „Cybernetic Capitalism: Information, Technology and Everyday Life", The Political Economy of

Kim Deok-hyun, (2001): 120,000 Internet Sites Blacklisted. In *Korea Times*, máj. 21.
Ko Shu-ling, (2001): Internet cafe proprietors protest „unfair" regulations. In *Taipei Times*, jún. 14.
Körmendy-Ékes Judit (2000): Az állam, a jog és az internet. In *Magyar Hírlap*, december 7., 7.
Lal Pai, Uday (2001): The Indian Government Wants to Regulate Interne. In *asia.Internet.com*, ápril. 18.
Latrive, Florent (2001): Le „cybermachin", pas encore né, déjà décrié: L'organisme français de régulation du Net sera créé en juin. In *Liberation,* febr. 21.
Launet, Edouard (2001): Piratage au sommer à Davos. In *Libération,* febr. 2. péntek.
Le CSA veut contr ler les images et les sons du Net. In *Vnunet.fr*, 2001. máj. 31.
Luening, Erich (2000): European council moves Net crime treaty forward. In *CNET News.com*. november 20., 3:35 p. m. PT.
Lyon, David (1994): The Electronic Eye: The Rise of Surveillance Society. Minneapolis.
MacKinnon, Richard (1997): Punishing the Persona: Correctional Strategies for the Virtual Offender. In *Virtual Culture: Identity and Communication in Cybersociety.* London.
Matt, Loney (2001): EU votes to restrict cookies. In *ZDNet (UK)*, november 13., 9:34 a. m. PT.
McCullagh, Declan (2000): Police Treaty a Global Invasion? In *Wired*, okt. 17., 3:00 p. m. PDT.
Rockenbauer Nóra és Újvári Miklós (2001): Európai Szövetségi Köztársaság vagy valami más? In *Magyar Hírlap*, május 17., 8.
Saussure, Ferdinad de (1972): *Cours de linguistique générale.* Paris.
Sieber, Ulrich (1998): *Legal Aspects of Computer-Related Crime in the Information Society*. Würzburg.
Sobchack, Vivian (1995): New Age Mutant Ninja Hackers: Reading „*Mondo 2000".* In Flame Wars: The Discourse of Cyberculture. Mark Dery (szerk.). Durham.
Stephens, Jon (2001): Has the EU Lost Its Mind? In *BuilderBuzz*, nov. 5., 12:33 a. m. PT.
Sterling, Bruce (1994): The Hacker Crackdown: Law and Disorder on the Electronic Frontier. Part 4. gopher://tic.com
Taggart, Stewart (2001): Questioning the Oz Net Censors. In *Wired News*, április 24.